ABSTRACT OF THE DISCLOSURE

A method and apparatus for Montgomery multiplication comprising adding at least one multiplicand bit from a first multiplicand add multiplexer in a main array of a Montgomery multiplier with at least one modulus bit from a first modulus-add multiplexer in the main array; adding at least one modulus bit from a first modulus-add multiplexer in a quotient pre-calculation array with at least one modulus bit from a second modulus-add multiplexer in the quotient pre-calculation array; pre-calculating the quotient during a first cycle; and sending at least one value to control the first modulus-add multiplexer in the main array, the first modulus-add multiplexer in the quotient pre-calculation array, and the second modulus-add multiplexer in the quotient pre-calculation array so that the value of the quotient is evenly divisible by the radix during a second cycle through the Montgomery multiplier.